REC'D 24 OCT 2005
WIPO PCT

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 54567PCT KMC:PFB	**FOR FURTHER ACTION**	See Form PCT/IPEA/416
International application No. **PCT/AU2004/000762**	International filing date *(day/month/year)* 10 June 2004	Priority date *(day/month/year)* 11 June 2003

International Patent Classification (IPC) or national classification and IPC

Int. Cl.[7] H04L 9/32, G06K 9/62

Applicant

THE COMMONWEALTH OF AUSTRALIA et al

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 4 sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:
   a. [X] *(sent to the applicant and to the International Bureau)* a total of **8** sheets, as follows:
      - [X] sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).
      - [ ] sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.

   b. [ ] *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s)) , containing a sequence listing and/or table related thereto, in computer readable form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).
4. This report contains indications relating to the following items:

[X]	Box No. I	Basis of the report
[ ]	Box No. II	Priority
[ ]	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
[ ]	Box No. IV	Lack of unity of invention
[X]	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
[ ]	Box No. VI	Certain documents cited
[ ]	Box No. VII	Certain defects in the international application
[X]	Box No. VIII	Certain observations on the international application

Date of submission of the demand	Date of completion of the report
8 April 2005	30 September 2005
Name and mailing address of the IPEA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized Officer **Mani Ramachandran** Telephone No. (02) 6283 2233

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/AU2004/000762

Box No. I Basis of the report

1. With regard to the language, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.

   ☐ This report is based on translations from the original language into the following language , which is the language of a translation furnished for the purposes of:

   ☐ international search (under Rules 12.3 and 23.1 (b))

   ☐ publication of the international application (under Rule 12.4)

   ☐ international preliminary examination (under Rules 55.2 and/or 55.3)

2. With regard to the elements of the international application, this report is based on (*replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report*):

   ☐ the international application as originally filed/furnished

   ☒ the description:

   pages **1-14** as originally filed/furnished
   pages* received by this Authority on with the letter of
   pages* received by this Authority on with the letter of

   ☒ the claims:

   pages as originally filed/furnished
   pages* as amended (together with any statement) under Article 19
   pages* **15-22** received by this Authority on **8 April 2005** with the letter of **8 April 2005**
   pages* received by this Authority on with the letter of

   ☒ the drawings:

   pages **1-3** as originally filed/furnished
   pages* received by this Authority on with the letter of
   pages* received by this Authority on with the letter of

   ☐ a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing.

3. ☐ The amendments have resulted in the cancellation of:

   ☐ the description, pages
   ☐ the claims, Nos.
   ☐ the drawings, sheets/figs
   ☐ the sequence listing (*specify*):
   ☐ any table(s) related to the sequence listing (*specify*):

4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

   ☐ the description, pages
   ☐ the claims, Nos.
   ☐ the drawings, sheets/figs
   ☐ the sequence listing (*specify*):
   ☐ any table(s) related to the sequence listing (*specify*):

* *If item 4 applies, some or all of those sheets may be marked "superseded."*

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/AU2004/000762

Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-41	YES
	Claims		NO
Inventive step (IS)	Claims	1-37, 40, 41	YES
	Claims	38, 39	NO
Industrial applicability (IA)	Claims	1-41	YES
	Claims		NO

2. Citations and explanations (Rule 70.7)

NOVELTY & INVENTIVE STEP Claims 1-41:

None of the citations disclose, alone or in an obvious combination, a credential communication device that performs mutual credential verification and mutual trusted recognition with another such credential communication device when in close physical proximity as to exclude third party involvement in the transmission and reception of data. Claims 1-37 are thus novel, and have an inventive step.

Claims 38, 39 is directed to a portable tamper resistant trusted device that is adapted to be used for personal identification and credential exchange and incorporates a wireless network interface, an inductive connector and trusted input switches and light displays. The term "trusted" implies employing sufficient hardware and software integrity measures to allow for processing a range of sensitive and classified information. The closest prior art of US 6058304 A (CALLAGHAN et al) 2 May 2000, discloses a handheld device having an integral sensor, control, storage, display means with a wireless telecommunications interface known to perform capturing, processing, storage, display and transmission of data. The ability to ensure "trusted" communication, with hardware and software integrity to protect from subversion, distinguishes the present invention and provides it with necessary inventiveness.

None of the citations, alone or in an obvious combination, anticipate the invention or render to lack an inventive step. The claimed invention is thus novel and inventive.

The claim does not limit such device to perform mutual credential verification and mutual trusted recognition with another such device when in close physical proximity as to exclude third party involvement in the transmission and reception of data. As seen in US 6058304 A (CALLAGHAN et al) 2 May 2000, a handheld device having an integral sensor, control, storage, display means with a wireless telecommunications interface is known to perform capturing, processing, storage, display and transmission of data. An ability to incorporate some kind of credential exchange capability as used in swipe cards or RFID tags, into such a device, would be well within the skill set of the addressee, as of the priority date. Inductive connectors and wheel press buttons, are mere mechanical integers of the device. They do not serve to characterise the inventive concept, and their presence into the device is not the outcome of the use of inventive ingenuity. I thus find claims 38 and 39 to lack an inventive step.

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1. The invention defined in claims 38, 39 is not supported by the description. The inventive concept is directed to a credential communication device that performs mutual credential verification and mutual trusted recognition with another such device when in close physical proximity as to exclude third party involvement in the transmission and reception of data. These features are conspicuously absent from claims 38 and 39.

CLAIMS

1. A credential communication device adapted to transmit and receive data, including means to process said data in order to effect mutual credential verification and trusted mutual recognition between the device and a second credential communication device, without reference to a third party, further including at least one proximity conductor adapted to be controlled to transmit and receive at least some data only when in such physical proximity to a second credential communication device as to effectively exclude the possibility of third party involvement in the transmission and reception of said data.

2. A credential communication device as in claim 1, further adapted to require a user of the device to authenticate their identity to the credential communication device immediately before communication with the second credential communication device.

3. A credential communication device as in claim 1or claim 2 further adapted to accept identity authentication by the keying of a pass code into the device.

4. A credential communication device as in claim 1or claim 2 further adapted to accept identity authentication by use of a biometric authentication apparatus.

5. A credential communication device as in any one of the preceding claims wherein the proximity connector is an induction connection.

6. A credential communication device as in claim 5, wherein the induction connection is effected by a RF transceiver of such power as to

require the physical proximity to be such as approximates physical touch.

7. A credential communication device as in any one of the preceding claims wherein there are means to effect variation in the power output of the proximity conductor in relation to the data to be transmitted wherein in use selected data, which is data whose unauthorised reception is acceptable, is transmitted at such power as to be received by the second credential communication device before said physical proximity to the second credential communication device as to effectively exclude the possibility of third party involvement in the transmission and reception of data is established, and other selected data, which is data whose unauthorised reception is not acceptable, is transmitted at such a power as to be received only when the credential exchange device is in such physical proximity to a second credential exchange device as to effectively exclude the possibility of third party involvement in the transmission and reception of data.

8. A credential communication device as in any one of the preceding claims wherein the proximity conductor includes means to detect that physical touch is being maintained between the device and a second device, the device further adapted to transfer some data only when such touch is detected.

9. A credential communication device as in claim 8 wherein the means to detect physical touch is a pressure sensor.

10. A credential communication device as in any one of the preceding claims wherein the proximity connector is protected from physical or environmental damage by a thin layer or shell of material.

11. A credential communication device as in any one of the preceding claims including means to communicate the results of processing to effect credential verification.

12. A credential communication device as in claim 11 wherein said communication means includes at least one trusted light indicator.

13. A credential communication device as in claim 11 wherein said communication means includes at least three separately identifiable trusted light indicators.

14. A credential communication device as in any one of claims 11-13 wherein said light indicators are formed as bands around the device to facilitate visibility from multiple angles.

15. A credential communication device as in any one of claims 11-14 wherein said light indicators are light emitting diodes.

16. A credential communication device as in any one of the preceding claims further including a trusted alpha-numeric display.

17. A credential communication device as in any one of the preceding claims further including a biometric authentication apparatus.

18. A credential communication device as in claim 17 wherein said biometric authentication apparatus is a fingerprint scanner.

19. A credential communication device as in any one of the preceding claims further including means for receiving wireless transmissions from a distance further than the range of the proximity conductor.

20. A credential communication device as in any one of the preceding claims wherein the device is approximately cylindrical and the proximity conductor is located on the shaft of said approximately cylindrical structure, permitting momentary contact with a second device from a variety of angles.

21. A credential communication device as in any one of the preceding claims wherein the proximity conductor is a bulbous structure, permitting momentary contact with a second device from a variety of angles.

22. A credential communication device as in any one of the preceding claims wherein the device is a component in a mutually authenticated ensemble of devices, the device being adapted to effect data display on a trusted remote visual display device.

23. A credential communication device as in claim 22 wherein the remote visual display device is a badge display.

24. A set of devices where a first of the devices is adapted to hold information in an electronic storage and effect transmission of such information upon a triggering of such transmission, and a second device is adapted to hold data in an electronic storage and adapted to receive transmissions from said first device and effect a comparison of such received data with that being held by said second device and when such received data is matching preselected criteria effect an output signal to this effect, the respective devices being adapted to effect a transmission and receiving of data between the devices only when in a selected range of distance apart or when touching, said devices being adapted to effect mutual credential verification, the devices being further adapted such that they will transmit and receive at least some data only when in such physical proximity as to effectively exclude the

possibility of third party involvement in the transmission and reception of data.

25. A method for mutual suspicion credential exchange including the steps of:

positioning a credential exchange device as in any one of claims 1-23 to touch or come into close proximity with a second such device,

the credential exchange device transmitting data to and receiving data from the second device,

the credential exchange device processing received data to determine the credential status of the second device,

the credential exchange device outputting the results of the credential determination.

26. A method for mutual suspicion credential exchange including the steps of:

providing each participant with a credential exchange device as in any one of claims 1-23,

loading the credential exchange device with credential data relevant to a user,

each participant operating their device to seek appropriate credential data from a second device,

each participant positioning their device to touch or come into close proximity with a second device,

each device transmitting data to and receiving data from a second device,

each device processing received data to determine the credential status of the second device,

each device outputting the results of the credential determination.

27. A method as in any one of claims 25-26 further including the steps of communicating an organisational mandatory security policy to

the credential exchange device, and the device applying said mandatory security policy to the data transmitted to the second device.

28. The method of claim 27 wherein the communication of the organisational mandatory security policy is restricted to being a one-off process performed when the device is manufactured or first activated.

29. The method of any one of claims 25-28 further including the steps of communicating a user discretionary security policy to the credential exchange device, and the device applying said user discretionary security policy to the data transmitted to the second device.

30. The method of claim 29 wherein the communication of the user discretionary security policy is restricted to being a one-off process performed when the device is manufactured or first activated.

31. The method of claim 27 wherein the mandatory security policy is communicated to the credential communication device by means localised to the particular location in which the device is operating.

32. The method of claim 31 wherein said policy communication is by secure wireless means.

33. The method of any one of claims 25-32 including the step of the credential communication device signalling via secure wireless means to a remote visual display means in its own ensemble a visual depiction of the participant associated with the second device.

34. A method for rapid verification of the credentials of a group of participants by a guard including the steps of:
providing each participant and the guard with a credential communication device as in any one of claims 1-23,

loading each participant's credential communication devices with data including the identity and credentials of the participant,
operating the guard's device to cause it to seek appropriate identity or credential data from a participant's device,
positioning each participant's device to touch or come into close proximity with the guard's device,
transmitting data and receiving data between the guard's and the participant's devices,
the guard's device processing received data to determine the credential status of the participant's device,
the guard's device outputting the results of the credential determination.

35. The method of claim 34 further including the step of providing a passive device adapted to extend the area in which proximity to the guard's device is sufficient for the proximity conductor to operate.

36. The method of claim 35 wherein the passive device is a waveguide, adapted to allow the guard's credential communication to be inserted into it, further including the step of each participant passing their credential communication device through the waveguide to communicate their credentials.

37. The method of any one of claims 34-36 wherein the guard's device is a component in an ensemble including a remote visual display device and further including the step of the guard's credential communication device signalling via secure wireless means to the remote visual display means in its own ensemble a visual depiction of the participant associated with the participant's device.

38. A portable tamper resistant trusted device adapted to be used for personal identification, credential warrants, and credential exchange including an inductive connector, one or more trusted input switches,

one or more trusted light displays to permit viewing from multiple angles, a trusted display, an untrusted wheel press button, an untrusted audio generator, and a wireless network interface.

39. A device as in claim 38 wherein the display is untrusted.

40. A credential communication device substantially as described with respect to any one of the embodiments in the specification with reference to and as illustrated by the accompanying illustrations with respect to that embodiment.

41. A method for mutual suspicion credential exchange substantially as described with respect to any one of the embodiments in the specification with reference to and as illustrated by the accompanying illustrations with respect to that embodiment.